The HIPAA Implementation Newsletter

Issue #45 – Friday, November 1, 2002

| Privacy | Security|

Web format with links at http://lpf.com/hipaa

Privacy: A Special Case

Reality has a way of testing our plans when we least expect it. The Washington area sniper case provides a special case for patient privacy – one that may provide a lesson for your planning. From the Washington Post: "The boy was admitted to Children's as a VOV -- victim of violence. For his protection, he was assigned an alias, which became the name all staffers would use, and which anyone seeking information about him would have to know. A bogus file was created in the computer system to throw potential hackers off the trail. And in this high-profile case, because the boy was considered a witness and therefore at risk, uniformed police officers stayed within reach of him at all times. Hospital security and admissions clerks at both entrances also were told to be on alert. The ER was locked down."
+ More at: http://www.washingtonpost.com/wp-dyn/articles/A37514-2002Oct16.html

Privacy: Compliance Officers

"The Health Care Compliance Association (HCCA) present the *5th Annual Survey - 2002 Profile of Health Care Compliance Officers*. …In just three years, health care organizations having active programs in place shot up from 55% in 1999 to 87% in 2002.

"The breadth of knowledge regarding compliance continues to grow within organizations, as does the hands-on experience and tenure of the current Corporate Compliance Officers. In 2002, there are five times as many Corporate Compliance Officers (44%) who have been on the job three-plus years as were able to make that claim 1999 (just 8%).

"The challenge to compliance programs nationwide of addressing HIPAA Privacy Regulations continues. Not only did 68% in 2002 say that HIPAA is the biggest issue their program faces, but 89% identified HIPAA being a specific program goal.

"About nine in every ten organizations (89%) provide regular training updates… Training is offered annually in the vast number of cases (79%) and sometimes more frequently (16%). However, there appears to be room for more training especially since most workers receive either one to three hours of training per year (in 48% of the organizations) or less than one hour (in another 41%). In-person classroom instruction by the Compliance Officer (76%) or another instructor (60%) is still the norm for Compliance Awareness Training. Video training has been deployed by 53%, and 46% are using computer/Web-based methods.

“The number of organizations having stand-alone compliance departments is up to 63% overall, and is actually higher than that in all but the smallest organizations. A majority of the compliance officers (56%) report directly to the CEO, or to the Board (another 10%).

“… departmental budget growth leveled this past year. Budget understandably aligns with the size of the organization, but the trends in this case indicate that “the poor are getting poorer”. Compliance budgets went down for the second straight year in the under 1,000 employee group … – a 10% drop from last year and down 22% from the average in 2000. … In contrast, the largest organizations (5,000 plus employees) budgeted … only 1% down from last year’s average.”
+ More at: http://www.hcca-info.org/documents/HCCAsurvey9_02.pdf

Security: Policies that Work

A recent study on information security policy has been made available on the Internet. Highlights include: “Policy forms the foundation of an information security solution, but many organizations struggle to turn documented policy into reality. … Although information security continues to have a high corporate profile, many organizations focus all their energies on searching for technological silver bullets. But implementing security technology without policy guidance is analogous to having police, courts, judges, and jails, but no law. Indeed, policy derived from business requirements is a prerequisite for effective information security….

“Our research indicates that most written security policy within Global 2000 organizations is ineffectual because it tends to be developed independently of the business. Security policy must constitute the business requirements to protect information resources.

“The primary problem with policy compliance results from the monolithic structure of typical policy documentation. The nature of the documentation prevents effective dissemination and communication. Providing the documentation in electronic format (e.g., on an intranet) does not in itself facilitate improved compliance.

“Our research indicates a structured hierarchy of policy classes enables more flexibility in policy development, evolution, and communication In addition, our research indicates the following set of best-practice principles that facilitate policy awareness and compliance:

- Policy should be derived from business requirements (and their associated risk implications). It must balance protection with productivity.
- Policy should be owned by the information resource owners and developed with the security team within the context of clearly understood roles and responsibilities. Ultimate accountability for policy enforcement should also rest with the information owners.

- Policy should be written concisely, unambiguously, and simply to ensure the target audience understands its responsibilities — where practical, the “language” (i.e., technical and functional terminology) of the target audience should be used.
- Policy should contain active sentences (i.e., it should indicate clear action and responsibility rather than vague objectives).
- Policy enforcement models should be linked to HR policy, employment contracts, job responsibility models, and disciplinary codes.
- Policy should be implementable and enforceable. Unenforceable (and unenforced) policy creates contempt. If policy cannot be enforced via technology, detection of non-compliance via audit and control procedures is an absolute minimum requirement.
- Policy definition and enforcement should be matched to organizational culture and structure. Depending on “self enforcement” in an authoritarian organization is bound to fail, as is rigorous top-down enforcement in a devolved, unstructured organization.

The report provides additional detail and figures to illustrate a “structured policy framework.” Available from: http://www.bindview.com/policywp/ Registration required.

Security: Percent of IT Budget

“Meta Group research indicates that companies will increase their IT security spending next year, defying the current downtrend in IT spending. Meta attributes the increase to cyber-terrorism threats and the pressure on CIOs to develop security and privacy architectures. Meta said more than half of the companies it studied will spend more than 5% of their IT budgets on security, up more than 20% from last year's study.”
From: SEARCHSECURITY.COM | Security and Industry News Oct. 29, 2002

Security: Top 20 Vulnerabilities

“The majority of the successful attacks on operating systems come from only a few software vulnerabilities. This can be attributed to the fact that attackers are opportunistic, take the easiest and most convenient route, and exploit the best-known flaws with the most effective and widely available attack tools. They count on organizations not fixing the problems, and they often attack indiscriminately, scanning the Internet for any vulnerable systems.

"While experienced security administrators will find the Top Twenty to be a valuable resource in their arsenal, the list is especially intended for those organizations that lack the resources to train, or those without technically-advanced security administrators. The individuals with responsibility for networks in those organizations often report that they have not corrected many of these flaws because they simply do not know which vulnerabilities are most dangerous, they are too busy to correct them all, or they do not know how to correct them safely. The SANS/FBI Top … includes step-by-step instructions and pointers to additional information useful for correcting the security flaws."
+ More at: http://www.sans.org/top20/

Security: Passwords

We see frequent admonitions about the need for strong passwords, but most authors fail to distinguish between material that deserves password protection and material that simply uses a password for identification and access. Does anyone really care if someone else pretends to be me and accesses my free subscription to a news Web site? Do I really have to have a password that is long, includes upper and lower case letters and a number or two? After all, most of these sites want people to read what they have to say. Failure to make a distinction between valuable material and just identification leaves the reader resisting good advice the same way we resist the good advice of an overly righteous uncle. That is probably part of the reason "… weak passwords are number seven on the SANS Institute/FBI's list of top 20 vulnerabilities released October 17, 2002.

SANS and the FBI specifically target access to operating systems and applications – it is easy to understand why they are worth protecting. They explain the issues and provide solutions including a list of three password cracking tools your security administrators can use to test your current passwords. (They also point out the need to get written approval. Cracking passwords is for professional drivers on closed courses only.) They provide explanations that any manager who uses a computer can understand and make action oriented recommendations on how to protect your enterprise. We encourage you to link to their side and read about passwords.

+ More at: http://www.sans.org/top20/#W7

Security: Event Management

“A ‘security event’ refers to any intrusive threat that will potentially impact the integrity of an organization’s computer files. In terms of the healthcare industry, these files may include patient files, databases, and other critical information protected by HIPAA.

Maintaining the confidence of patients as well as the trust of physicians and business partners oftentimes relies on maintaining the privacy and integrity of the trusted information. Internal fraud and unauthorized access are real threats to information security. While healthcare institutions must protect the confidentiality of personally identifiable health information to comply with regulation, the integrity of personal information is paramount for effective and timely care. Unfortunately, many organizations will find the preparation of HIPAA audit information time consuming and burdensome. Internal team overloads will lead to lack of focus, unmanageable business volumes, and IT needs can fall by the wayside.

Additionally, with information technology attacks (hackers, viruses, etc.) on the rise, there are increasing business risks involved with operating networked systems.

Oftentimes, healthcare organizations lack the ability to measure and report on security performance and policy enforcement. This is another key area of need in the information technology department.

Finally, a lack of systems integration often poses significant problems for healthcare organizations. Because systems for healthcare organizations typically run in a multi-vendor environment, any number of systems and software solutions may be used in the everyday operations that make the business flow. In the event of a security attack, many organizations find they do not have the capabilities to protect information across a wide range of vendor systems.

A real-time threat management solution … can expose key threats and identify weak links in an organization’s security environment while enabling policy enforcement and reducing mountains of data to a manageable amount. Some of the business impacts of implementing an effective real-time threat management solution include:

- Preventing and/or mitigating breaches against critical business processes, protecting data integrity and ensuring availability while reducing downtime
- Systematically exposing weak links in security infrastructures, enacting technologies, policies, or processes to fortify those links

- Increasing security team efficiency by focusing on critical threat response, enforcing policy, and fortifying key assets, all while reducing the time spent on laborious tasks such as automated log monitoring and responding to false positives
- Preventing and/or stopping attacks before they impact critical business systems
- Preventing unauthorized access to patient information
- Mitigating risk of electronic fraud

+More at:
http://www.esecurityinc.com/productcorporateliterature/whitepapers/HIPAA.pdf

Security: Guidelines for the Security Certification and Accreditation

NIST sets the standards for the administrative wing of the federal government and they have just released a new set of guidelines for public comment. They set specific standards for and define responsibility for the security of systems being developed and those in operation. This may be a "heads-up" of what to expect from HHS's security regulations.

"This special publication establishes a standard process, general tasks and specific subtasks to certify and accredit IT systems ... While [it] … focuses on federal IT systems, the associated tasks and subtasks, security controls, and verification techniques and procedures, have been broadly defined so as to be universally applicable to all types of IT systems … Ensuring that appropriate security objectives are developed and that the security risks are identified and balanced against operational demands is a fundamental management responsibility.

The authorization of an IT system to process, store, or transmit information, granted by a management official, provides a form of quality control and challenges managers and technical staff to find the best fit for security, given technical constraints, operational constraints, and mission requirements [defined here as] … *accreditation*. The technical and non-technical evaluation of an IT system that produces the necessary information required by the authorizing official to make a credible, risk-based decision on whether to place the system into operation is known as *certification*.

The Designated Approving Authority (DAA) is a senior management official or executive with the authority to formally approve the operation of an IT system at an acceptable level of risk. … These officials have the authority to oversee and influence the budget and business operations of the systems … In addition to having the authority to approve systems for operation, **the DAA has the authority to disapprove systems for**

operation and, if the systems are already operational, the authority to halt operations if unacceptable security risks exist. … [Emphasis added]

The *program manager* and *system owner* represent the interests of the user community and the IT system throughout the system's life cycle. The program manager is responsible for the system during initial development and acquisition and is concerned with cost, schedule, and performance issues. The system owner assumes responsibility for the system after delivery and installation during operation, maintenance, and disposal.

For operational systems, the *system security officer* is responsible for the day-to-day security of a specific IT system including physical security, personnel security, incident handling, and security awareness, training, and education. …For developmental systems, the system security officer serves as the principal technical advisor to the program manager for all security-related issues.
+ More at: http://csrc.nist.gov/sec-cert/SP-800-37-v1.0.pdf

To be removed from this mail list, click: mailto:hipaa@lpf.com?subject=remove

To subscribe, click: mailto:hipaa@lpf.com?subject=subscribe We appreciate it if you include information about your firm and your interests.

The HIPAA Implementation Newsletter is published periodically by Lyon, Popanz & Forester. Issues are posted on the Web at http://lpf.com/hipaa concurrent with email distribution. Past issues are also available there. Edited by Hal Amens hal@lpf.com

Information in the HIPAA Implementation newsletter is based on our experience as management consultants and sources we consider reliable. There are no further warranties about accuracy or applicability. It contains neither legal nor financial advice. For that, consult appropriate professionals.

Lyon, Popanz & Forester http://lpf.com is a management consulting firm that designs and manages projects that solve management problems. Planning and project management for HIPAA are areas of special interest.